C4ISRNET

NETWORK REQUIREMENTS FOR ARMY 2030

Sponsored by:

paloalto NETWORKS

A U.S. Army Staff Sgt. confers with his replicated foreign partner counterpart during an exercise testing Army 2030 operations.

SPC. HANS WILLIAMS/U.S. ARMY

NETWORK REQUIREMENTS FOR ARMY 2030

By: Andrew Welsh-Huggins

As the United States Army develops its Army of 2030 initiative — the service's biggest reorganization and technical upgrade since the Cold War — a reliable and effective cybersecurity network infrastructure that turns raw data into actionable intelligence is required to meet the program's modernization goals.

To build that infrastructure, the Army in particular and the Department of Defense in general will need a redesigned, whole-network approach, with a focus on getting data to and from the tactical user quickly and reliably to allow for data-driven decision-making, a goal that fits into a larger services-wide initiative known as Joint All-Domain Command and Control (JADC2). Analyzing threats in real-time to protect the network and to guard against data loss and malware are key components of this initiative and the Army of 2030's cybersecurity planning.

All this will require a major transition in priorities especially given the enormous amount of data available for analysis and the growing importance of artificial intelligence and machine learning, said Jim Smid, the DoD/Intel Field chief technology officer at Palo Alto Networks, a Santa Clara, California-based global cybersecurity firm.

'Just scratching the surface'

"Warfighting is not just done with tanks and airplanes and conventional weaponry," said Smid, whose company in November warned of "an unprecedented level" of cybersecurity attacks. "There's so much that's happening from a cybersecurity perspective."

The Army in 2030 needs to be a lot nimbler than it currently is, Smid continued.

"They need to be able to take advantage of a lot of data, a lot of cross-correlation," he said. "They need to be really keeping track of artificial intelligence, machine learning, and integrating a lot more automation and workflows into their day-to-day warfighters."

The reality, Smid added, is that officials are "just scratching the surface" in terms of what more needs to be done in the cybersecurity realm, and how.

Recent testimony before Congress underscored the challenge the Defense Department faces in this area given the fact it gathers at least

22 terabytes of data each day, an undertaking that makes data-driven analysis of all that information more important than ever. Without the proper tools to interpret that data, the information is essentially lost in the ether and useless to warfighters, a long-standing problem when organizations implement Security Information and Event Management (SIEM) systems, according to Smid, who noted that a lot of data simply isn't being used.

In October, the Army summarized the issue in its Field Manual FM 2-0, noting that intelligence needs to encompass the entire operational environment.

"Intelligence professionals must understand the land, maritime, air, space, and cyberspace domains as well as the human, information, and physical dimensions to be effective," the report said.

Data's outsized military services role is something that experts at the DoD's Data Science Directorate (DSD) have continuously focused on since the DSD's inception six years ago, DSD leaders said at an October anniversary summit.

"Everyone is realizing the importance of data," Lt. Col. Nick Lee, NETCOM DSD data scientist, said at the forum. "Everything is data-driven."

Quantum computing

In addition to the artificial intelligence tools needed to interpret all this data, the reality of quantum computing—the ability to perform multiple calculations at the same time—is also on the horizon, as is the ability to encrypt data and transmissions. The gold standard is "near real-time intelligence," Smid said, without which it's not possible to identify and respond to alerts and dangerous situations. In other words, it all comes down to what's known as mean time to detect (MTTD), or the time it takes for an existing problem to be identified.

Speakers discussed how the Army of 2030 will fight in a GPS denied and degraded environment at the AUSA Global Force Symposium & Exposition 2023.

PATRICK HUNTER/U.S. ARMY

"If you run a query and you have to come back a day and a half later to find out what happened, it's too late," Smid said.

As a result, achieving near real-time intelligence means a major paradigm shift for how the Army will operate the cybersecurity side of its house, said Smid, whose company looks at more than one trillion flow logs a day. Palo Alto Networks also features a threat response wing, dubbed Unit 42, which offers security consulting and threat intelligence services, and recently launched the industry's first integrated Code to Cloud intelligence platform. In October, Palo Alto Networks added to its cloud security portfolio by buying Israeli security firm Dig Security, six months after acquiring another Israeli firm, Talon Cyber Security, a secure web browser start-up company.

Outpacing adversaries

The military's new emphasis on upgrading cybersecurity comes as the Army implements its Army of 2030 initiative, a program — under the umbrella of the Army's 2021 Digital Transformation Strategy — meant to ensure that the U.S. won't be outpaced by adversaries whether on traditional battlefields, in cyberspace, or in the new military frontier of space. A key element is being able to reliably communicate and share data within Army divisions, its sister services, and military coalition partners.

The introduction of each new system increases the Army's ability to respond to threats and be a deterrent to adversaries, Christine Wormuth, the Secretary of the Army, said in a keynote address at the Association of the U.S. Army Annual Meeting and Exposition in Washington, D.C. in October.

"We must continue to embrace innovation and transformation or risk failing to address future threats," Wormuth said.

Congress has taken note of the pressing need to improve data security.

The U.S. Senate Committee on Armed Services, in its proposed version of the National Defense Authorization Act for 2024 released in July, called on the DoD to make identity, credential, and access management (ICAM) tools — an essential part of the cybersecurity verification process known as Zero Trust — an official program of record.

"An enterprise-wide ICAM capability is a critical and pressing need for the Department of Defense (DOD) not only for cybersecurity but also for managing complex multi-domain military operations involving information and systems classified at multiple levels," the committee said in a report.

One of the lessons of recent contested environments in places like Iraq and Afghanistan was the military's ability to obtain data from unorthodox sources, such as measuring spikes in cellular activity via cell phone towers that corresponded with military action.

Those discoveries underscored that an evolving cyber-security strategy is part of redefining warfare, particularly in an environment where cyber-attacks now rank at the same threat level as conventional assaults, Smid said.

"If you can knock out some of the defenses or something as simple as some of the cameras, the physical security, things like that, if that's coordinated with everything else and you can knock out the ability of your adversary to take advantage of some of the data that's out there and some of their telemetry and their systems, that's a critical part of being successful in the war," Smid said. A report by Palo Alto Network's Unit 42 in November underscored this threat, as it said it had identified a Chinese Advanced Persistent Threat (APT) infrastructure masquerading as a cloud backup service that was maliciously targeting Cambodian government agencies.

U.S. Soldiers assigned to 3rd Security Force Assistance Brigade, pull security for a UH-60 Black Hawk helicopter during an Army 2030 exercise.

SPC. MOLLY MORROW/U.S. ARMY

Achieving the upgrade necessary to obtain these capabilities will require a wholesale approach, since — as Smid puts it — pulling a thread in one area uncovers other places needing continuous improvement especially when it comes to sharing data between disparate systems and applications. In addition, because the services rely on multiple legacy systems, a reluctance exists to admit that it's time to modernize and replace a system.

As a result, building an upgraded infrastructure comes first, followed by improvements in the integration, correlation, and sharing of data. "People are going to have to continue to invest in what the new capabilities are," Smid said. The first step will be upgrading the older, legacy systems, whether adding things like quantum encryption capabilities or new tools for data analysis through artificial intelligence and machine learning.

"A rising tide floats all boats," Smid said. "And that will certainly be true from the infrastructure standpoint. You're going to have to make some investments across the board to make sure that everything is kind of up to snuff."

Looking towards Zero Trust

Looking farther down the road, the better job the services can do controlling the data they receive, the more the network becomes a less critical part of the overall structure, a move away from the era of "classified networks" and "unclassified networks."

This is important whether warfighters are on a base or in the field, particularly in the age of Zero Trust, the cyber security strategy that requires individuals or entities accessing resources, even within a network, to be verified every time, even if they've previously been cleared. Zero Trust, along with data centricity, mission partner environments, interoperability,

and defensibility, are foundational concepts of CJADC2 key to execute globally integrated operations around the world, Col. Anne-Marie Wiersgalla, SouthCom communications director, said at the annual AUSA conference (the 'C' or 'combined' of the moniker adds allies to the concept of creating a common platform for sharing data).

A report by Research and Markets estimated the U.S. JADC2 market value at $1.2 billion in 2023 and as much as $8.6 billion by 2030. In November alone, the Air Force made 13 additional awards to develop technologies for its JADC2 sector, known as the Advanced Battle Management System (ABMS).

Smid emphasized that having robust Zero Trust capabilities in place has never been more important, especially given that some of the biggest data breaches within federal government systems in the past decade have been internal attacks, not external ones.

"You should have the same look and feel," Smid said, adding that consolidating the number of tools at hand always makes things simpler. "You should have the performance that you're anticipating, and you should certainly have the same degree of security, regardless of where you're coming from."

One year ago, the Department of Defense released its Zero Trust Strategy and Roadmap. The agency noted that current and future cyber threats require a Zero Trust approach that extends beyond the traditional perimeter defense approach. The department cited three goals for its roadmap, to be implemented by Fiscal Year 2027: reducing the attack surface; enabling risk management and effective data-sharing in partnership environments; and quickly containing and remediating adversary activities.

"Implementing Zero Trust will be a continuous process in the face of evolving adversary threats and new technologies," the department said in November 2022.

Yet this implementation underscores the challenges that lie ahead when it comes to cybersecurity upgrades since zero trust is more than just a product. Rather, it represents an ecosystem of products working together to ensure that devices, applications, users, the network, and more, all have the same capability, said Smid, who added that the Army recognizes that current tool sets haven't adequately addressed Zero Trust as a concept. In addition, Zero Trust integration gaps exist and further policies and procedures regarding Zero Trust still need to be adapted, Smid said.

"There's all kinds of things that are going to go into making sure that you're making good mission-critical decisions along the way," he said. Consistency is key, he added.

"You should certainly have the same degree of security, regardless of where you're coming from."

– **Jim Smid,**
DoD/Intel Field Chief Technology Officer,
Palo Alto Networks

"You want to make sure that, whether you are remote or whether you're on base, that your cybersecurity is handled the same way, your network infrastructure is handled the same way," Smid said.

The systems that the Department of Defense adopts must also adhere to DoD standards, which means partnering with the services and being open about existing gaps in security and how they can be best addressed.

"I think the most critical thing that I've heard from our DoD customers, when it comes to Zero Trust, is 'Don't tell us that you can do everything right. Be honest, be a partner with us,'" Smid said.

Finally, all Zero Trust tools must embrace the concepts of automation and orchestration, the two pillars of the security system's philosophy. "If you don't take those last two pillars and infuse them into everything else you do from a Zero Trust capability, you won't be successful in the long run," Smid said.

These capabilities are central to CJADC2 and its goal of making sure that reliable data that can be acted upon is put in the hands of warfighters. To accomplish this, the DoD must move away from past security environments to one where each person's access and clearance is verified, Scott St. Pierre, the Navy Director of Enterprise Networks and Cybersecurity, said during an October panel discussion organized by GovCIO Media & Research.

"In order to find the right balance, we have to start treating, and have been since 2006, cybersecurity as a key system attribute of the design of every system we deliver," St. Pierre said. "What we're doing now with things like JADC2 is we're taking a step back and looking at it at the enclave level and the platform level as opposed to it just at the individual system level."

On the heels of the need to fully integrate Zero Trust into the services' cybersecurity portfolio is the necessity of developing quantum-ready encryption, or encryption that could prevent an attack by hostile entities, including the possibility, down the road, of certain nation-states using quantum computers, Smid said. Ensuring that encryption is in place is an intensive process involving infrastructure upgrades and ratifying

standards for addressing encryption and quantum computing.

“Between Zero Trust and quantum-ready encryption, those are probably two of the top priorities I see coming up over the next few years,” Smid said.

At the core of any conversation about a major cybersecurity upgrade, of course, especially one dominated by talk of hardware and software, is the role of personnel. Smid believes it’s not feasible for the services to go on a massive hiring spree, but instead, the focus should be on training.

After all, not only is automation not going away, it is impossible to run a Security Operations Center (SOC) without having automation orchestration, artificial intelligence, and machine learning. The whole idea after all, as Smid says, is that not only should personnel be getting smarter, but machines should too — being taught to do something a second time, for example, after a process has been accomplished initially. This is especially crucial so that, when detecting data anomalies, the difference between an attack and a normal transaction can be distinguished.

“And that’s what happens a lot in cybersecurity, you can get overwhelmed by the noise that isn’t important, and you can miss the signal that was a critical event,” Smid said. “So being able to have tools that will help you sort through that and make those good decisions is all about making your personnel better at their jobs.” The key, then, is helping the workforce become more efficient and providing tools that help warfighters and people doing cybersecurity distinguish between a signal and noise.

“The whole idea of cybersecurity is you wake up the next day and you’re smarter than you were the day before,” Smid added. “You know more about what the attacks are than the day before.” C4